INFORMATION SECURITY MANAGEMENT: WHY THE EMERGING ISO 27000 SERIES ARE VITAL FOR BUSINESS RESILIENCE

Vernon Poole

Many readers will remember the early days of BS7799 when efforts were made to establish a UK Code of Practice on Information Security Management. From 1989 onwards, attempts were made to convert this standard into an international standard – ISO 17799 and it soon became obvious that, as information security threats and vulnerabilities grew, an acceptable global standard ISO 27001 would emerge. ISO 27001 was the first move by the ISO community to align Information Security Management with the Quality Management standard – ISO 9001. There is now an ISO 27000 series of standards that you need to be aware of, and this article outlines their progress/emergence and how they will be valuable tools to adopt.

ISO 27000 SERIES - INTRODUCTION
The initial family of ISO 27000 series covered the following seven areas:

- ISO 27000 – Fundamentals and vocabulary (under development)
- ISO 27001 – ISMS requirements (BS7799 – Part 2)
- ISO 27003 – ISMS Implementation Guidance (under development)
- ISO 27004 – ISMS Metrics and measurement (under development)
- ISO 27005 – ISMS Risk Management (under development)
- ISO 27006 – Guidelines on ISMS accreditation for certifiers

The initial aspect for you to understand is that:
ISO 27001 is the certification process to gain compliance or certification,
ISO 27002 is the Code of Practice (11 guiding principles; 133 detailed controls)

The other 27000 series are additional guides/advisory areas to assist organisations to establish a consistent framework on Information Security Management – the emphasis is on ‘Information Security’ not ‘IT’ because of the wider Governance requirements. There is now developments on Auditing (ISO 27007) and other guidance will be added over time. A key development will be the emergence on sector specific guides.

These seven areas can be viewed pictorially as:

Structure of 27000 series

<table>
<thead>
<tr>
<th>27000 Fundamentals &amp; Vocabulary</th>
</tr>
</thead>
<tbody>
<tr>
<td>27001: Information Security Management System (ISMS)</td>
</tr>
<tr>
<td>27002 Code of Practice for ISM</td>
</tr>
<tr>
<td>27003 Implementation Guidance</td>
</tr>
<tr>
<td>27004 Metrics &amp; Measurement</td>
</tr>
<tr>
<td>27006 Guidelines on ISMS accreditation</td>
</tr>
</tbody>
</table>

ISO 27000 SERIES – IN DETAIL

1. ISO 27000 FUNDAMENTALS & VOCABULARY

This standard will address the following issues:

- explains the terminology for all the 27000 series family of standards
- addresses global concerns on definitions that vary from country to country – so consistency will be established
- these principles will impact on other standards like COBIT (IT Processes) and ITIL (IT Service Delivery) and avoid any confusion.

The clarity that ISO 27000 will bring should not be underestimated. The number of times that debate/arguments takes place between organisations (especially in an outsourced environment) or professional bodies on various terms like network security or risk assessment can be eliminated forever.

Publication date for this standard is scheduled for 2009.

2. ISO 27001 INFORMATION SECURITY MANAGEMENT SYSTEM (NOVEMBER 2005)

This standard allowed for certification to the Code of Practice (ISO27002) w.e.f. 30 January 2006. Clearly, for many, compliance is as far as most organisations are proceeding at present. There is however, an emerging scheme where organisations can seek ‘advanced compliance’ where the ISMS framework is reviewed annually by a third party.

The standard clarifies/improves PDCA process requirements, namely:

- ISMS scope
- Approach to risk assessment
- Selection of controls
- Statement of Applicability
- Reviewing risks
- Management commitment
- ISMS internal audits
- Results of effectiveness & measurements
- Update risk treatment plans/procedures controls

The demand for ISO certification is currently growing at the rate of 150 organisations per month – there are now 4,000
certifications with over 1,000 new certifications in the last 12 months (previous certifications were up to BS7799 – 2 status though many have been upgraded consequently). This growth can be attributed to many factors but the overriding reason is that organisations are making this standard a contractual, regulatory (e.g. e-gov directive) or service level agreement requirement – which is leading to a major reason for its take-up. This take-up is across both private & public sectors. Therefore, you need to monitor the ISO certification website – www.iso27001certification and be aware of which organisations are becoming certified in their sector.

3. ISO 27002 CODE OF PRACTICE FOR INFORMATION SECURITY MANAGEMENT (JULY 2007)

This standard replaces ISO/IEC 17799:2005 and covers the following:

- 11 sections specify 39 control objectives to protect information assets
- Provides 133 best practice controls that can be adopted based on a risk assessment process – but leaves an organisation free to select controls not listed in the standard – giving great flexibility in implementation (but challenging for certification bodies!)
- Standard is updated every three years and the most recent changes cover:
  - security of external service delivery & provisioning of outsourcing
  - patch management
  - security prior to, during and at termination of employment (HR controls)
  - guidance on risk management,
  - a section on incident management
  - mobile, remote & distributed communications

ISO27002 is now deployed as the global de-facto standard.

4. ISO 27003 IMPLEMENTATION GUIDANCE

This standard will utilise the Appendix that was attached to the former BS7799-2 which covers:

- overview
- management responsibilities
- governance & regulatory compliance
- personal security & human resources
- asset management
- availability/continuity of business processes
- handling information incidents
- access control
- risk management case studies

Publication date for this standard is scheduled for 2009

5. ISO 27004 METRICS & MEASUREMENT

This standard is aimed at addressing how to measure the effectiveness of ISMS implementations (processes and controls)

- Performance targets
- What to measure

How to measure
- When to measure

The measurement programme objectives are to:

- Evaluate the effectiveness of security controls & control objectives;
- Evaluate the effectiveness of the ISMS inc. continual improvement;
- Provide security indicators to assist management review
- Facilitate improvement of information security
- Provide input for security audits;
- Communicate the effectiveness of ISM to the organization;
- Serve as an input into the risk management process
- Provide output for internal comparison & benchmarking of effectiveness

Publication date for this standard is scheduled for 2008

6. ISO 27005 RISK MANAGEMENT

This is a new standard on ‘Information Security Risk Management. This requirement has been a thorn in the side of many organisations who have been going for ISO27001 certification, because, for most organisations information security risk management is either very poor or not recognised from a Corporate Risk Register perspective. Therefore, this standard is eagerly awaited; the following outline explains how the standard will be developed:
8. ADDITIONAL ISO 27000 SERIES STANDARDS BEING DISCUSSED
- ISO 27007 Guidelines for ISMS Auditing

This standard will provide guidance for audit and accredited certification bodies auditing ISMS – it will draw heavily on ISO 19011:2002 (the ISO standard for auditing quality and environmental management systems).
Publication date for this standard will not be until 2009 (currently not scheduled)

- ISO 27011 ISM Guidelines for Telecommunications

Publication date for this standard will probably be 2010.

There are other sector specific guides being considered for: Lottery; Automotive; & Finance sectors.

- ISO 27031 ICT readiness for Business Continuity
- ISO 27032 Guidelines for Cybersecurity
- ISO 27033 IT Network Security
- ISO 27034 Guidelines for Application Security

No publication dates yet for these specific guides

- ISO 27799 Security Management in Health using ISO27002 (draft)

This standard is currently being discussed because of its alignment issue.

CONCLUSION

Organisations can see that there is a wealth of valuable guidance being prepared which is gaining global acceptance on a consistent approach to Information Security Management issues. This guidance will assist you in helping your organisation to adopt best practice or identify benefits/obstacles to implementing them.

AUTHOR

Vernon Poole – Head of Business Consultancy, Sapphire

The views expressed in this article are based on the author’s experience in deploying these standards over 17 years. The author is willing to receive comments or provide further information via vernon.poole@sapphire.net

Vernon is Head of Business Consultancy, responsible for Sapphire’s team of consultants who deal with Information Assurance and all best practice standards on Information Security Management and associated areas (ISO27000 series; ITIL; COBIT; ValIT).

Vernon began his career in consultancy with CAPITA and has over 20 years experience in information security management consultancy and training.